应用离散数学

杭州电子科技大学

代数结构

1 代数运算

2 代数系统

3 半群与群

4 子群和陪集

5 循环群

定义16 (子群)

设$\langle G, * \rangle$是群，H是G的非空子集。若H对于运算$*$也构成群，则称H是G的子群。

- $G, \{e\}$是G的子群，被称为平凡子群。
- 如$\langle \mathbb{Z}, + \rangle$是$\langle \mathbb{Q}, + \rangle$的子群。
- $\langle \mathbb{Z}_6, +_6 \rangle$有哪些子群？

定理8 (子群的判定1)

设$\langle G,*\rangle$是群，H是G的非空子集，则H是G的子群的充要条件是

1. $\forall a\in H, a^{-1}\in H$
2. $\forall a,b\in H$，$a*b\in H$

定理9 (子群的判定2)

设$\langle G,*\rangle$是群,H是G的非空子集，则H是G的子群的充要条件是

$$\forall a,b\in H, a*b^{-1}\in H$$

例14

若$\langle G,*\rangle$是群，$\forall a\in G$，则$H=\langle a\rangle=\{a^k|k\in\mathbb{Z}\}$是$G$的子群，被称为由$a$生成的子群。

例15

设$\langle G,*\rangle$是群，令C是G中与G中所有元素都可交换的元素构成的集合，即

$$C=\{a|a\in G\wedge\forall x\in G(a*x=x*a)\}$$

则C是G的子群，被称为G的中心。

例4.19

设$\langle G, * \rangle$是群，H, K都是G的子群，证明

1. $H \cap K$是G的子群；
2. $H \cup K$是G的子群的充要条件是$H \subseteq K$或$K \subseteq H$

定义17 (陪集)

设$\langle G,*\rangle$是群，H是其子群。对于$a\in G$，称

- $aH=\{a*h|h\in H\}$为H相应于a的左陪集
- $Ha=\{h*a|h\in H\}$为H相应于a的右陪集

注2

- 一般情况下，左、右陪集并不相等；
- 当G是交换群时，左、右陪集相等；

例17 (已知$\langle\mathbb{Z}_6,+_6\rangle$是群，求子群$\{0,2,4\}$所有的陪集。)

定理10

设$\langle G, * \rangle$是群，H是G的子群，定义G上的二元关系

$$R = \{\langle a, b \rangle | a \in G \wedge b \in G \wedge b^{-1} * a \in H\}$$

证明

1. R是G上的等价关系；
2. $[a]_R = aH$；

定理11

设$\langle G,*\rangle$是群，H是其子群，则H的所有左陪集构成G的划分，即

- $\forall a,b\in G$，有$aH=bH$或$aH\cap bH=\emptyset$
- $\bigcup\limits_{a\in G}aH=G$

定理12

设$\langle G,*\rangle$是群，H是其子群，则$\forall a,b\in G$，有

1. $a\in bH\Leftrightarrow b^{-1}*a\in H\Leftrightarrow aH=bH$
2. $a\in Hb\Leftrightarrow a*b^{-1}\in H\Leftrightarrow Ha=Hb$

定理13

设$\langle G,*\rangle$是群，H是其子群，则$\forall a\in G, H\sim aH, H\sim Ha$。

定义18 (指数)

群$\langle G,*\rangle$的子群H的左(右)陪集组成集合的基数被称为H在G中的指数，记为$[G:H]$。

定理14 (拉格朗日定理)

设$\langle G,*\rangle$是有限群，H是其子群，则$|G|=[G:H]\times|H|$。特别地$|H|\big||G|$。

推论 (设$\langle G,*\rangle$是n阶群，$a\in G$，则)

1. $a^n=e$;
2. $|a|$是n的因子;
3. 若n是质数，则存在$a\in G$，使得$G=\langle a\rangle$，即质数阶群都是循环群。

作业　习题4.4 第1，2，4，5题

定义19 (循环群)

设$\langle G,*\rangle$是群，若$\exists a\in G$，使得$\forall x\in G$,都有$x=a^k,k\in\mathbb{Z}$，则称$\langle G,*\rangle$是循环群，a是其生成元，记为$G=\langle a\rangle$。

注3

1. 若$|a|=n$，则$G=\langle a\rangle=\{e,a^1,a^2,\cdots,a^{n-1}\}$
2. 若a是无限次元，则$G=\langle a\rangle=\{e,a^{\pm1},a^{\pm2},\cdots\}$
3. 循环群必定是交换群
4. 若$G=\langle a\rangle,|a|=n$，则$|G|=n$
5. 若$\langle G,*\rangle$是n阶有限群，$a\in G$且$|a|=n$，则$\langle G,*\rangle$必定是循环群，且a是生成元

定理15

设$G=\langle a\rangle$是循环群，$a^0=e$是单位元，则

1. 若a是无限次元，即$G=\{e,a^{\pm1},a^{\pm2},\cdots\}$，则$G$中只有$2$个生成元$a,a^{-1}$
2. 若$|a|=n$，即$G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，则$a^k,1\leq k\leq n$是生成元的充要条件是

$$\gcd(k,n)=1$$

即G中只有$\varphi(n)$个生成元，其中$\varphi(n)$表示$[1,n]$中与n互质的整数个数

例19 (求出以下各个循环群所有的生成元)

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}_7^*, \times_7 \rangle$
3. 循环群$G = \{e, a, a^2, \cdots, a^{14}\}$

例4.25

设G是n阶循环群，$\forall m \in \mathbb{Z}, m|n$，则必定存在$a \in G$，使得$|a| = m$

作业 习题4.5 第 3，4 题